HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 200310819-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Boon Ho et al.

Confirmation No.: 8413

Application No.: 10/717521

Examiner: Feben Haile

Filing Date: Nov. 21, 2003

Group Art Unit: 2416

Title: Method and System For Monitoring A Network Containing Routers Using A Backup Routing Protocol

Mail Stop Appeal Brief - Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF REPLY BRIEF

Transmitted herewith is the Reply Brief with respect to the Examiner's Answer mailed on Oct. 22, 2008 .

This Reply Brief is being filed pursuant to 37 CFR 1.193(b) within two months of the date of the Examiner's Answer.

(Note: Extensions of time are not allowed under 37 CFR 1.136(a))

(Note: Failure to file a Reply Brief will result in dismissal of the Appeal as to the claims made subject to an expressly stated new ground rejection.)

No fee is required for filing of this Reply Brief.

If any fees are required please charge Deposit Account 08-2025.

Respectfully submitted,
Boon Ho et al.

By: /Mary Jo Bertani/
Mary Jo Bertani
Attorney/Agent for Applicant(s)
Reg No. : 42321
Date : Dec. 22, 2008
Telephone : 949-350-7301

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Boon Ho et al.		
Assignee:	Hewlett-Packard Development Company, L.P.		
Title:	Method and System For Monitoring A Network Containing Routers Using A Backup Routing Protocol		
Serial No.:	10/717521	Filing Date:	Nov. 21, 2003
Examiner:	Feben Haile	Group Art Unit:	2416
Docket No.:	200310819-1	Confirmation No.:	8413

Irvine, California
December 22, 2008

MAIL STOP APPEAL BRIEF
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

REPLY BRIEF

Dear Sir:

This Reply Brief is submitted in response to the Examiner's Answer dated October 22, 2008.

I. Real Party in Interest

The present application is assigned to Hewlett-Packard Development Company, L.P. Hewlett-Packard Development Company, L.P is the real party in interest, and is the assignee of Application No.1 0/717,521.

II. Related Appeals and Interferences

The Appellant legal representative, or assignee, does not know of any other appeal or interferences which will affect or be directly affected by or have bearing on the Board's decision in the pending appeal.

III. Status of Claims

The claims currently pending in this application are claims 1-37, all of which stand finally rejected. Claims 1-37 are being appealed.

IV. Status of Amendments

No Amendments were filed after final rejection.

V. Summary Claimed Subject Matter

Pursuant to 37 C.F.R. §41.37(1)(c)(v) , the subject matter of independent claims 1, 12, 24 and 35 on appeal are cross-referenced to the specification and/or drawing figures in the following table. The following table is not to be construed as a representation that the portions of the disclosure identified below constitute the sole basis for support of the claimed subject matter.

Claim	Disclosure
1. A method for monitoring a network containing routers using a backup routing protocol and organized in at least one backup router group, comprising:	Lines 1 and 2, para. [0025]; lines 1-3, para. [0033]; Fig. 1.

discovering a topology object model of the routers;	Line 3, para. [0025]; lines 4 and 5, para. [0033]; 102 of FiG.1.
detecting a condition of the at least one backup router group based on at least one threshold value; and	Lines 3 and 4; para. [0025]; lines 9 and 10 of para. 0033; 104 of FiG. 1.
displaying an indication of the detected condition.	Line 5, para. [0025]; lines 10 and 11, para. [0033]; 106 of Fig.1 .
12. A system for monitoring a network containing routers using a backup routing protocol and organized in at least one backup router group, comprising:	Lines 1 and 2, para. [0026]; lines 1 and 2, para. [0053]; Fig. 3
means for discovering a topology object model of the routers and detecting a condition of the at least one backup router group based on at least one threshold value; and	Lines 3-5, para. [0026]; lines 3 and 4, para. [0053]; 330 of Fig. 3
means for displaying an indication of the detected condition.	Line 5, para. [0026]; lines 6 and 7, para. [0053]; 310 of Fig. 3
24. A computer readable medium comprising a computer program embedded therein for causing a computer to perform:	Lines 5-7 para. [0025]; lines 12-14, para. [0067]; Fig. 3.
discovering a topology object model of routers included within a network;	Line 3, para. [0025]; lines e para. [0067]; 330 of Fig. 3
detecting a condition of at least one backup router group of the routers based on at least one threshold value; and	Lines 3 and 4, para. [0025]; line 4, para. [0067]; 330 of Fig. 3
displaying an indication of the detected condition.	Line 5, para. [0025]; lines 9 and 10, para. [0067]; 310 of Fig. 3
35. A data structure embodied within a computer readable medium for Representing a backup routing protocol topology object model for a network, the data structure comprising:	Lines 1 and 2, para. [0027]; lines 1-3, para. [0049]; 200 of Fig. 2.
at least one network node object representing an element in the network;	Lines 3 and 4, para. [0027]; line 4, para. [0049]; 204 of Fig. 2.
at least one network interface object for each at least one network node object, the at least one network interface object representing an interface of	Lines 4 and 5, para. [0027];

the network element corresponding to the each at least one network node object;	Lines 4-6, para. [0049]; 206 of Fig. 2.
an address object for each at least one network interface object, representing an address of the corresponding interface;	Lines 6 and 7, para. [0027]; lines 8 and 9, para. [0049]; 212 of Fig. 2
a backup routing protocol group object representing network elements organized in a backup routing protocol group, the backup routing protocol group object including a virtual address of the backup routing protocol group and real addresses of the network elements in the backup routing protocol group; and	Lines 8-11, para. [0027] lines 10-12, para. [0049]; 202 of Fig. 2.
an address state object for each of the real addresses of the network elements in the backup routing protocol group, including a state of the corresponding address.	Lines 11-13, para. [0027]; lines 19 and 20, para. [0049]; 216 of Fig. 2.

VI. Grounds of Rejection to be Reviewed on Appeal

The final Office Action presents the following grounds of rejection to be reviewed on appeal:

A. Claims 1, 3-6, 8-12,14-17,19-24,26-29 and 31-36 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Application Publication US 2004/0083284 A 1 (Ofek et al.), in view of U.S. Patent 7,197,660 (Liu et al.).

B. Claims 2, 7, 13, 18, 25 and 30 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Application Publication US 2004/0083284 A1 (Ofek et al.), in view of U.S. Patent 7,197,660 (Liu et al.), and in view of U.S. Patent 6,954,436 (Yip et al.).

VII. Argument

Claims 1. 3-6. 8-1 2. 14-17. 19-24. 26-29 and 31-36

Claims 1. 3-6. 8-1 2. 14-17. 19-24. 26-29 and 31-36 stand rejected under 35 U.S.C. §103{a) as being unpatentable over U.S. Patent Application Publication US 2004/0083284 A1 (Ofek et al.) in view of U.S. Patent 7,197,660 (Liu et al.).

In numbered paragraph 3, pages 2-11 of the final Office Action, the Examiner has rejected claims 1,3-6,8-12,14-17,19-24,26-29 and 31-36 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Publication No. US 2004/0083284 (Ofek et al.) in view of U.S. Patent No. 7,197,660 (Liu et al). This rejection is respectfully traversed, as the documents relied upon by the Examiner fail to teach, suggest or provide any motivation whatsoever for Appellants' invention as set forth in independent claims 1, 12, 24 and 35. While the Office Action Summary sheet enumerates all of claims 1-37 as being rejected, there is no explicit statement of Examiner's rejection directed to dependent claim 37.

The Examiner has failed to establish a prima facie case of obviousness in combining the Ofek et al. publication with the Liu et al. patent to reject independent claims 1, 12, 24 and 35. For example, Appellants' independent claim 1 method recites, among other features, discovering a topology object model of routers, and detecting a condition of at least one backup router group based on at least one threshold value. Claim 1 also recites displaying an indication of the detected condition. Such features are neither taught nor suggested by the documents relied upon by the Examiner, such that claim 1 is allowable. Because the other independent claims recite various aspects of features discussed with respect to claim 1, these claims are also allowable.

More particularly, in rejecting claim 1 on pages 2 and 3 of the final Office Action, the Examiner refers to paragraph [0021] of the Ofek document. On page 3 of the final Office Action, the Examiner acknowledges the Ofek document "fails to explicitly suggest detecting a condition of the at least one backup router group based on at least one threshold value". However, the Examiner asserts that it would have

been obvious to "incorporate the recovery method taught by Liu into the system for providing data awareness disclosed by Ofek". This assertion of the Examiner is respectfully traversed. Appellants respectfully disagree with the Examiner's ultimate conclusion. Even assuming, arguendo, that a motivation to combine is somehow interjected as suggested by the Examiner, the presently claimed invention would not have resulted.

The Ofek et al. publication is directed to using a topology object model (e.g., para. (0021)) to store elements of different types of domains (e.g., the SONET-based domain and the DWDM-based domain mentioned in paragraph [0004] of the Ofek et al. publication). There is no discussion in the Ofek et al. publication of configuring a network to contain routers that use a backup routing protocol, and that are organized in at least one backup router group. As such, there is no teaching or suggestion in the Ofek publication of any mechanism for discovering topology information concerning such routers, or for evaluating conditions of such routers. The Ofek et al. publication therefore fails to provide teaching or suggestion of detecting a condition of at least one backup router group based on a threshold value, as presently recited in Appellants' claim 1. Because there are no routers which use a backup routing protocol that are discovered in the Ofek publication, and no detecting of any condition associated with a backup router group containing such routers, the Ofek publication also fails to disclose or suggest the claim 1 feature of displaying any indication of such a detected condition.

The Liu et al. patent is directed to a network security system wherein a master device and backup device within a cluster of network security devices are provided. The Liu patent describes detecting failure in the cluster of network security devices, and using the state information to recover from the failure (abstract). The Liu et al. patent shows in Fig. 2 a recovery system 202 which has a memory 208 and a controller 206. Memory 208 contains a redundancy group table 210, a master data partition 212 and a backup data partition 214. Each security device 102 is assigned to one or more redundancy groups and each redundancy group is assigned to host a certain set of connections. Within each redundancy group, one security device is designated the master, another security device is designated the primary backup, and the remaining security devices in the redundancy group are designated as

secondary backups (col. 4, lines 21-30). However, this disclosure of "security device" in the Liu et al. patent does not relate specifically to routers that use a backup routing protocol, and do not disclose at least one backup router group. As such, there is no teaching or suggestion in the Liu et al. patent of any mechanism for discovering topology information concerning such routers or backup router groups, or for evaluating conditions of such routers.

The Liu et al. patent further discloses "a path monitor 228 which detects failures of other devices within the cluster 110 (i.e., not local failures). The Examiner appears to take out of context the mention of a path monitor 228 containing a failure threshold parameter that defines the threshold for what constitutes a "failure" for other devices or paths in the system (col. 5, lines 17-25). However, at least for the reasons as set forth above, this "threshold" disclosure of the Liu et al. patent that the Examiner relies on is not specifically related to detecting a condition of at least one backup router group based on a threshold value, as presently recited in Appellants' claim 1.

The Liu et al. patent mentions a redundancy group so that a "next master" can be pre-selected before a failure occurs in the network affecting the originally identified master device (col. 8, lines 10-29). However, this again relates to "security devices". There is no teaching or suggestion in the Ofek et al. publication or in the Liu et al. patent of detecting a condition of a backup router group based on a threshold value, and displaying an indication of such a detected condition as part of a network monitoring operation (see Appellants' claim 1). (Emphasis added). The Ofek et al. publication and the Liu et al. patent do not relate to backup router groups. Further, the Liu et al. patent does not deal with display of backup router group information. Further, neither document deals with detecting and displaying conditions of a backup router group. Instead, the Liu et al. patent determines the condition of individual devices and links between devices (col. 5 lines 17-25).

As such, claim 1 is allowable over the documents relied upon by the Examiner.

The remaining independent claims 12, 24 and 35 recite features similar to those discussed with respect to claim 1 and are also allowable. For example, claim

12 recites a system for monitoring a network wherein a discovering means discovers a topology object model of routers using a backup routing protocol, and detecting a condition of at least one backup router group based on a threshold value; and displaying an indication of the detected condition. Independent claim 24 is directed to a computer readable medium containing similar features. Independent claim 35 is directed to a data structure for representing a backup routing protocol topology object model for a network. The data structure includes, among other features, a backup routing protocol group object. Such a feature enables an exemplary embodiment wherein conditions of a backup routing group can be detected and displayed. For reasons similar to those discussed with respect to the remaining independent claims, claims, 12, 24 and 35 are also allowable.

The remaining rejected claims 3-6, 8-11, 14-17, 19-23, 26-29, 31-34, and 36 depend from the respective one of the aforementioned independent claims, and recite additional advantageous features which further distinguish over the documents relied upon by the Examiner.

For at least these reasons, the rejection of claims 1, 3-6, 8-12, 14-17, 19-24, 26-29 and 31-36 is improper. Accordingly, the rejection should be reversed.

Claims 2, 7, 13, 18, 25 and 30

Claims 2, 7, 13, 18, 25 and 30 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Application Publication US 2004/0083284 A 1 (Ofek et al.), in view of U.S. Patent 7,197,660 (Liu et al.), and in view of U.S. Patent 6,954,436 (Yip et al.)

On pages 11-17 of the final Office Action, the Examiner has rejected claims 2, 7, 13, 18, 25 arid 30 under 35 U.S.C. § 103(a) as being unpatentable over the Ofek et al. publication in view of the Liu et al. patent, and in further view of U.S. Patent No. 6,954,436 (Yip et al.). This rejection is respectfully traversed, as the documents relied upon by the Examiner fail to teach, suggest or provide any motivation whatsoever for Appellants' invention as set forth in subject claims.

Appellants have set forth arguments submitting that the Ofek et al. publication and the Liu et al. patent do not teach or suggest features recited in independent

claims 1, 12, 24 and 35. Appellants respectfully submit that the Yip et al. patent does not cure the deficiencies of the Ofek et al. publication and/or the Liu et al. patent.

The Yip et al. patent relates to electing a master router in a virtual router network by obtaining a tracking parameter for each of the routers participating in a virtual router network (abstract). However, the passages that the Examiner relies on merely describe a first tracking parameter based on a number of successful pings of IP addresses that respond that they are alive and capable of receiving traffic from an SRP router (e.g., col. 4, lines 30-40). However, the Yip et al. patent fails to teach or suggest detecting a condition of a backup router group based on a threshold value, and displaying an indication of the detected condition as recited in Appellants' claim 1, and as similarly recited in independent claims 12, 24 and 35. Yip et al. patent, considered individually or in the combination with the Ofek et al. publication and the Liu et al. patent as the Examiner has suggested, fails to teach or suggest the benefits of a discovery process and a topology object model data structure, as variously recited in independent claims 1, 12, 24 and 35, which enables conditions of a backup router group to be detected and displayed for effective network management by a user.

Claims 2 and 7 depend from independent claim 1; claims 13 and 18 depend from independent claim 12; and claims 25 and 30 depend from independent claim 24, and include features that further distinguish them from the prior art. For example, claims 2, 13, and 25 recite "the at least one threshold value includes a minimum number of available routers in a backup router group." Claims 7 and 30 recite "the condition is a minimum number of functional routers available in a corresponding backup router group." One portion of Yip et al. cited as teaching these features in contrast describes a first tracking parameter based on a number of successful pings of IP addresses that respond that they are alive and capable of receiving traffic from an SRP router (e.g., col. 4, lines 30-40). Another cited portion of Yip et al. describes a third tacking parameter that is a diagnostic tracking parameter (col. 4 lines 50-51). The first tracking parameter in Yip et al. is not a threshold value that includes a minimum number of available routers in a backup router group. (Emphasis added). Similarly, the diagnostic tracking parameter of Yip et al. is not a minimum number of functional routers available in a corresponding

backup router group.

At least for these reasons, the documents relied upon by the Examiner fail to teach, suggest or provide any motivation whatsoever for Appellants' invention as set forth in subject claims, nor do the documents, alone or in combination, teach or suggest all of the features of the claims.

For at least these reasons, the rejection of claims 2, 7, 13, 18, 25 and 30 is improper. Accordingly, the rejection should be reversed.

Conclusion

The Examiner has failed to establish a prima facie case of obviousness in rejecting claims 1,3-6,8-12,14-17,19-24,26-29 and 31-36; and in separately rejecting dependent claims 2, 7, 13, 18,25 and 30. Further, while the Office Action Summary sheet enumerates dependent claim 37 as being rejected, there is no explicit statement of Examiner's rejection directed to dependent claim 37. At least for these reasons, a reversal of the final rejection, and allowance of the present application, are therefore requested.

VIII. Claims Appendix

See attached Claims Appendix for a copy of the claims involved in the appeal.

IX. Evidence Appendix

Evidence Appendix as attached indicates: NONE.

X. Related Proceedings Appendix

Related Proceedings as attached indicates: NONE.

VIII. CLAIMS APPENDIX

The Appealed Claims

1. A method for monitoring a network containing routers using a backup routing protocol and organized in at least one backup router group, comprising:

discovering a topology object model of the routers;

detecting a condition of the at least one backup router group based on at least one threshold value; and

displaying an indication of the detected condition.

2. The method of Claim 1, wherein the at least one threshold value includes a minimum number of available routers in a backup router group.

3. The method of Claim 1, wherein the detecting is also based on a number of backup router groups to which one of the routers belongs.

4. The method of Claim 1, wherein for each backup router group the topology object model comprises:

at least one network router node;

at least one network interface for each at least one network router node;

at least one address for each at least one network interface;

a state of each one of the at least one address that is internal to the backup router group; and

any tracked interfaces associated with each one of the at least one address that is internal to the backup router group.

5. The method of Claim 4, wherein the topology object model comprises:

a state of at least one of the at least one address that is external to the backup router group.

6. The method of Claim 5, wherein the detecting is also based on the state of the at least one address that is external to the backup router group.

7. The method of Claim 1, wherein the condition is a minimum number of functional routers available in a corresponding backup router group.

8. The method of Claim 1, wherein the condition is a minimum number of functional routers available only in a corresponding backup router group.

9. The method of Claim 1, comprising:

receiving status information from the routers; and

updating the topology object model to reflect the received status information.

10. The method of Claim 9, wherein the status information includes states associated with interface addresses within the at least one backup router group.

11. The method of Claim 10, wherein the status information includes status of

tracked interfaces associated with routers organized in the at least one backup router group.

12. A system for monitoring a network containing routers using a backup routing protocol and organized in at least one backup router group, comprising:

means for discovering a topology object model of the routers and detecting a condition of the at least one backup router group based on at least one threshold value; and

means for displaying an indication of the detected condition.

13. The system of Claim 12, wherein the at least one threshold value includes a minimum number of available routers in a backup router group.

14. The system of Claim 12, wherein the detecting is also based on a number of backup router groups to which one of the routers belongs.

15. The system of Claim 12, wherein for each backup router group the topology object model comprises:

at least one network router node;

at least one network interface for each at least one network router node;

at least one address for each at least one network interface;

a state of each one of the at least one address that is internal to the backup router group; and

any tracked interfaces associated with each one of the at least one address that is internal to the backup router group.

16. The system of Claim 15, wherein the topology object model comprises: a state of at least one of the at least one address that is external to the backup router group.

17. The system of Claim 16, wherein the detecting is also based on the state of the at least one address that is external to the backup router group .

18. The system of Claim 12, wherein the condition is a minimum number of functional routers available in a corresponding backup router group.

19. The system of Claim 12, wherein the condition is a minimum number of functional routers available only in a corresponding backup router group.

20. The system of Claim 12, comprising:

means for receiving status information from the routers and for updating the topology object model to reflect the received status information.

21. The system of Claim 20, wherein the status information includes states associated with interface addresses within the at least one backup router group.

22. The system of Claim 21, wherein the status information includes status of tracked interfaces associated with routers organized in the at least one backup router group.

23. The system of Claim 12, wherein:

the means for discovering also receives status information from the routers and updates the topology object model to reflect the received status information.

24. A computer readable medium comprising a computer program embedded therein for causing a computer to perform:

discovering a topology object model of routers included within a network;

detecting a condition of at least one backup router group of the routers based on at least one threshold value; and

displaying an indication of the detected condition.

25. The medium of Claim 24, wherein the at least one threshold value includes a minimum number of available routers in a backup router group.

26. The medium of Claim 24, wherein the detecting is also based on a number of backup router groups to which one of the routers belongs.

27. The medium of Claim 24, wherein for each backup router group the topology object model comprises:

at least one network router node;

at least one network interface for each at least one network router node;

at least one address for each at least one network interface;

a state of each one of the at least one address that is internal to the backup router group; and

any tracked interfaces associated with each one of the at least one address that is internal to the backup router group.

28. The medium of Claim 27, wherein the topology object model comprises:

a state of at least one of the at least one address that is external to the backup router group.

29. The medium of Claim 28, wherein the detecting is also based on the state of the at least one address that is external to the backup router group.

30. The medium of Claim 24, wherein the condition is a minimum number of functional routers available in a corresponding backup router group.

31. The medium of Claim 24, wherein the condition is a minimum number of functional routers available only in a corresponding backup router group.

32. The medium of Claim 24, wherein the computer program causes the computer to perform:

receiving status information from the routers; and

updating the topology object model to reflect the received status information.

33. The medium of Claim 32, wherein the status information includes states associated with interface addresses within the at least one backup router group.

34. The medium of claim 33, wherein the status information includes status of tracked interfaces associated with routers organized in the at least one backup router group.

35. A data structure embodied within a computer readable medium for representing a backup routing protocol topology object model for a network, the data structure comprising:

at least one network node object representing an element in the network;

at least one network interface object for each at least one network node object, the at least one network interface object representing an interface of the network element corresponding to the each at least one network node object;

an address object for each at least one network interface object, representing an address of the corresponding interface;

a backup routing protocol group object representing network elements organized in a backup routing protocol group, the backup routing protocol group object including a virtual address of the backup routing protocol group and real addresses of the network elements in the backup routing protocol group; and

an address state object for each of the real addresses of the network elements in the backup routing protocol group, including a state of the corresponding address.

36. The data structure of Claim 35, comprising:

a track interface object corresponding to a tracked network interface of a first network element in the backup routing protocol group wherein the tracked network interface is located between the first network element and a network element outside the backup routing protocol group.

37. The data structure of Claim 35, wherein:

the backup routing protocol group is related to one or more network node objects;

the backup routing protocol group is related to one or more address objects;

each network node object is related to one or more backup routing protocol group objects;

each network node object is related to one or more network interface objects;

each network interface object is related to one or more address objects; and

each address object is related to one or more network interface objects.

IX. EVIDENCE APPENDIX

NONE.

X. RELATED PROCEEDINGS APPENDIX

NONE.